Amendments to the Claims:

This listing of claims replaces all prior listings, and versions, of claims in the present application.

Listing of Claims:

1. (Currently Amended) A method for preventing unauthorized use of software accessing at least one specific hardware module comprising a unique hardware identification sequence wherein said software comprises a license key for being executed, comprising:

reading out said hardware identification sequence of said at least one specific hardware module, said reading out being performed at a processing device executing the software;

retrieving, at the processing device, a predetermined hardware identification sequence contained in said license key;

comparing, at the processing device, said read-out hardware identification sequence with said hardware identification sequence contained in the license key;

permitting execution of said software if both sequences match; and

wherein said hardware identification sequence contained in said license key is encrypted and a first secret key coded in said software is used to decrypt said hardware identification sequence, ~~and~~

wherein at least one of said specific hardware modules is a Bluetooth module comprising a unique Bluetooth hardware address that comprises said hardware identification sequence that is read out, and

wherein said first secret key is encrypted additionally using a public key encryption method, comprising:

a second secret key which is only known to a trusted third authority; and

a public key corresponding to said second secret key; and wherein said second secret key is used for encrypting said first secret key and said public key is used for decrypting said encrypted first secret key and wherein said public key is the only key which allows decrypting data encrypted by the second secret key.

2-7. (Canceled)

8. (Previously Presented) The method according to claim 22, wherein at least one of said specific hardware modules is a network interface module comprising a unique network interface address.

9. (Previously Presented) The method according to claim 8, wherein at least one of said specific hardware modules is a Bluetooth module comprising a unique Bluetooth hardware address.

10-16. (Canceled)

17. (Previously Presented) The method according to claim 21, wherein at least one of said specific hardware modules is a network interface module comprising a unique network interface address.

18. (Previously Presented) The method according to claim 22, wherein at least one of said specific hardware modules is a network interface module comprising a unique network interface address.

19. (Currently Amended) The method according to claim 22~~claim 6~~, wherein at least one of said at least one specific hardware modules is a network interface module comprising a unique network interface address.

20. (Canceled)

21. (Currently Amended) A method for preventing unauthorized use of software accessing at least one specific hardware module comprising a unique hardware identification sequence wherein said software comprises a license key for being executed, comprising:

reading out said hardware identification sequence of said at least one specific hardware module, said reading out being performed at a processing device executing the software;

retrieving, at the processing device, a predetermined hardware identification sequence contained
in said license key;

comparing, at the processing device, said read-out hardware identification sequence with said hardware identification sequence contained in the license key;

permitting execution of said software if both sequences match; and wherein said hardware identification sequence contained in said license key is encrypted and a secret algorithm coded in said software is used to decrypt said hardware identification sequence, wherein said secret algorithm is encrypted additionally using a public key encryption method, comprising:

a secret key which is only known to a trusted third authority; and

a public key corresponding to said secret key; and

wherein said secret key is used for encrypting said secret algorithm and said public key is used for decrypting said encrypted secret algorithm and wherein said public key is the only key which allows decrypting data encrypted by the secret key.

22. (Currently Amended) A method for preventing unauthorized use of software accessing at least one specific hardware module comprising a unique hardware identification sequence wherein said software comprises a license key for being executed, comprising:

reading out said hardware identification sequence of said at least one specific hardware module, said reading out being performed at a processing device executing the software;

retrieving, at the processing device, a predetermined hardware identification sequence contained in said license key;

comparing, at the processing device, said read-out hardware identification sequence with said hardware identification sequence contained in the license key;

permitting execution of said software if both sequences match; and

said hardware identification sequence contained in said license key is encrypted and a public key encryption method is used for encrypting and decrypting said unique hardware identification sequence contained in said license key, comprising a secret key which is only known to the license key distribution authorities; and a public key corresponding to said secret key; and wherein

said secret key is used for encrypting said hardware identification sequence and said public key is used for decrypting said hardware identification sequence and wherein said public key is the only key which allows decrypting data encrypted by the secret key, wherein said public key is encrypted additionally using a public key encryption method, comprising:

a second secret key which is only known to a trusted third authority; and

a second public key corresponding to said second secret key; and

wherein said second secret key is used for encrypting said public key and said second public key is used for decrypting said encrypted public key and wherein said second public key is the only key which allows decrypting data encrypted by the second secret key.

23. (Previously Presented) The method according to claim 21, wherein at least one of said specific hardware modules is a network interface module comprising a unique network interface address.

24. (Previously Presented) The method according to claim 23, wherein at least one of said specific hardware modules is a Bluetooth module comprising a unique Bluetooth hardware address.